All Entangled Quantum States Are Nonlocal

Francesco Buscemi*
Institute for Advanced Research, Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan
(Dated: 16 April 2012)

Departing from the usual paradigm of local operations and classical communication adopted in entanglement theory, here we study the interconversion of quantum states by means of local operations and shared randomness. A set of necessary and sufficient conditions for the existence of such a transformation between two given quantum states is given in terms of the payoff they yield in a suitable class of nonlocal games. It is shown that, as a consequence of our result, such a class of nonlocal games is able to witness quantum entanglement, however weak, and reveal nonlocality in any entangled quantum state. An example illustrating this fact is provided.

It is a fact that the outcomes of measurements performed on spatially separated (i.e. non-communicating) quantum systems sometimes exhibit correlations, which cannot be explained classically, in terms of information shared beforehand. Such correlations, called *nonlocal*, are revealed by the violation of a suitable Bell inequality [1, 2]. Another peculiarly nonclassical feature of quantum theory is the existence of *quantum entanglement*, i.e. the property possessed by composite quantum systems whose joint state cannot be written in product form (or, more generally, as a mixture of states in product form). Even if nonlocality and entanglement are indeed intimately related, it is nowadays widely accepted that they are in fact two well distinct concepts: first of all, because there exist entangled quantum states which behave "locally" in many aspects [3, 4]; second, because quantum states that appear to be "maximally nonlocal" are generally not the "maximally entangled" ones [5]. Such a quantitative distinction is made clear by looking upon nonlocality and entanglement as two *inequivalent resources*.

In the resource theory of quantum entanglement, the operational paradigm is commonly known as *local operations and classical communication* (LOCC) [6]: separated parties are only allowed to exchange classical messages, while quantum operations (i.e. preparation of quantum states, quantum measurements, etc.) can only happen locally. In particular, quantum states cannot be directly sent across separated locations. The LOCC paradigm, originally formulated in order to describe the "distant laboratories model", is nowadays generally accepted as the natural operational paradigm for studying quantum entanglement as a resource [7]: indeed, classical communication cannot generate entanglement, which hence becomes a physical resource that can be processed, but not created.

In a resource theory of nonlocality, on the other hand, the LOCC paradigm seems unjustified: even mere classical communication constitutes in fact a nonlocal resource and, as such, cannot be granted freely. For this reason, some authors consider the natural operational paradigm of nonlocality to be that of *local operations and shared randomness* (LOSR) [8]. (A notable exception to this argument occurs if nonlocality is measured in terms of *private* correlations: in this case, *public* classical communication can be freely allowed [9].) In the LOSR framework, separated parties are forbidden all sorts of communication, being allowed though to "synchronize" their local operations with respect to a common classical random variable shared in advance. Hence, nonlocal correlations being defined as those correlations that cannot be simulated by shared randomness [10], nonlocality naturally becomes a resource in the LOSR paradigm.

The resource theory of quantum entanglement, with respect to the resource theory of nonlocality, has received until now much more attention in the literature: correspondingly, many results are known about the interconversion of quantum states by LOCC transformations [7], while much less is known about the LOSR case [8]. The aim of the present letter is to contribute in bridging this gap, by providing a set of necessary and sufficient conditions for the existence of an LOSR protocol transforming one distributed quantum state into another. Such conditions, rather than algebraic, are *operational*, in the sense that they are expressed in terms of the payoffs that a quantum state yields in nonlocal games. More precisely, the main result of this letter is to show that one quantum state can be transformed into another by means of an LOSR protocol, if and only if the former yields a higher payoff than the latter for a whole class of nonlocal games, which we call *semi-quantum* nonlocal games. A remarkable merit of our analysis is to provide a simple and insightful proof of the fact that *all entangled quantum states are nonlocal* [11]: a corollary of our main result is that any entangled quantum state yields a strictly higher payoff than every separable state, in at least one semi-quantum nonlocal game. This general fact will be also illustrated in an explicit example, clarifying how semi-quantum nonlocal games are able to faithfully witness entanglement.

Nonlocality ordering.—In order to rigorously state the main result (Prop. 1 below), we first need to introduce some notation and few definitions. In what follows, all quantum systems are finite-dimensional (i.e. their Hilbert spaces, denoted by $\mathcal{H}$, are finite-dimensional) and

index sets (denoted by $\mathcal{S}$, $\mathcal{T}$, $\mathcal{X}$, and $\mathcal{Y}$) contain only a finite number of elements. The convex set of probability distributions defined on an index set $\mathcal{X}$ is denoted by $\mathscr{P}(\mathcal{X})$. The set of linear operators acting on a Hilbert space $\mathcal{H}$ is denoted by $\mathsf{L}(\mathcal{H})$. The set of density matrices (i.e. positive semi-definite, trace-one operators) is denoted by $\mathsf{S}(\mathcal{H}) \subset \mathsf{L}(\mathcal{H})$.

A random source of states of a quantum system A is represented by an ensemble $\tau = (\{p(s), \tau^s\}; s \in \mathcal{S})$, where $p \in \mathscr{P}(\mathcal{S})$ and $\tau^s \in \mathsf{S}(\mathcal{H}_A)$, for all s. Given an outcome set $\mathcal{X} = \{x\}$ and a quantum system A with Hilbert space $\mathcal{H}_A$, an $\mathcal{X}$-probability operator-valued measure ($\mathcal{X}$-POVM, for short) on A is a family $P = (P^x; x \in \mathcal{X})$ of positive semi-definite operators $P^x \in \mathsf{L}(\mathcal{H}_A)$, such that $\sum_{x\in\mathcal{X}} P^x = \mathbb{1}$. We denote by $\mathscr{M}(A; \mathcal{X})$ the convex set of all $\mathcal{X}$-POVMs on A. A POVM $P \in \mathscr{M}(A; \mathcal{X})$ induces, via the relation $p(x) = \mathrm{Tr}[P^x \varrho]$, a linear function $P : \varrho \mapsto P\varrho$ from $\mathsf{S}(\mathcal{H}_A)$ to $\mathscr{P}(\mathcal{X})$. POVMs in $\mathscr{M}(A; \mathcal{X})$ are used to model measurements performed on a quantum system A with outcomes in $\mathcal{X}$.

The notion of nonlocal games is of central importance in our discussion (we begin here by considering the bipartite case; the multipartite case follows directly and will be briefly discussed at the end of the paper):

Definition 1. The rules of a *nonlocal game* G_{nl} consist of the following: four index sets $\mathcal{S} = \{s\}$, $\mathcal{T} = \{t\}$, $\mathcal{X} = \{x\}$, and $\mathcal{Y} = \{y\}$; two probability distributions $p \in \mathscr{P}(\mathcal{S})$ and $q \in \mathscr{P}(\mathcal{T})$; a payoff function $\wp : \mathcal{S} \times \mathcal{T} \times \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$. A referee picks indices $s \in \mathcal{S}$ and $t \in \mathcal{T}$ at random with probabilities $p(s)$ and $q(t)$, and sends them separately to two players, say Alice and Bob, respectively. The two players, without communicating with each other, must compute answers $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively, and send them to the referee, who will then pay them both (i.e. the game is *collaborative*) an amount equal to $\wp(s, t, x, y)$. (It is understood that a negative payoff means a loss, i.e. the players must pay the referee.)

First, the players are told the rules of the game. Knowing the rules, the players are allowed to agree on any strategy and to share any possible (static) resource. Later on, the players and the referee agree to begin the game, and, from that moment on, an implicit rule of all nonlocal games forbids the players to communicate. According to quantum theory then, anything the two players can do is to share a bipartite quantum state $\varrho_{AB} \in \mathsf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and, depending on the questions s and t they are presented, perform independent measurements on A and B with values in $\mathcal{X}$ and $\mathcal{Y}$, respectively.

Imagine now that the state ϱ_{AB} shared between Alice and Bob is *fixed*. It is a well-defined question to ask "how good" is the state ϱ_{AB} for playing a given nonlocal game G_{nl}. In order to answer this question, it is convenient to use a mathematical model in which the referee communicates her questions to Alice and Bob by means of a quantum channel. This means that the referee, depending on which questions $s \in \mathcal{S}$ and $t \in \mathcal{T}$ she picked, prepares two auxiliary quantum systems A_0 and B_0, with dimensions $\dim \mathcal{H}_{A_0} \geqslant |\mathcal{S}|$ and $\dim \mathcal{H}_{B_0} \geqslant |\mathcal{T}|$, in the orthonormal states $\pi^s := |s\rangle\langle s|$ and $\pi^t := |t\rangle\langle t|$, and sends them to Alice and Bob, respectively. We suppose that the states are transmitted without noise. Since Alice and Bob exactly know which game they are playing and which state they are sharing, the payoff they expect to gain (on average) can be expressed by the following formula:

$$\wp^*\left(\varrho_{AB}; \mathsf{G}_{\mathrm{nl}}\right) := \max \sum_{s,t,x,y} p(s)q(t)\wp(s,t,x,y)\mu(x,y|s,t), \quad (1)$$

where $\mu(x, y|s, t)$ is the joint conditional probability distribution computed as

$$\mathrm{Tr}\left[(P^x_{A_0A} \otimes Q^y_{BB_0})(\pi^s_{A_0} \otimes \varrho_{AB} \otimes \pi^t_{B_0})\right],$$

and the maximization is performed over all POVMs $P \in \mathscr{M}(A_0A; \mathcal{X})$ and $Q \in \mathscr{M}(BB_0; \mathcal{Y})$.

The function $\wp^*(\varrho_{AB}; \mathsf{G}_{\mathrm{nl}})$ in (1) measures the "nonlocal utility" of ϱ_{AB} in playing a nonlocal game G_{nl}. Accordingly, if another state $\sigma_{A'B'} \in \mathsf{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ is such that $\wp^*\left(\sigma_{A'B'}; \mathsf{G}_{\mathrm{nl}}\right) \leqslant \wp^*\left(\varrho_{AB}; \mathsf{G}_{\mathrm{nl}}\right)$, we say that ϱ_{AB} is better than $\sigma_{A'B'}$ for playing G_{nl}. By extending this definition to *all* nonlocal games, we can introduce the following relation:

Definition 2. A bipartite state $\varrho_{AB} \in \mathsf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be (*definitely*) *more nonlocal* than another bipartite state $\sigma_{A'B'} \in \mathsf{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, written $\varrho_{AB} \succcurlyeq_{\mathrm{nl}} \sigma_{A'B'}$, if and only if $\wp^*\left(\varrho_{AB}; \mathsf{G}_{\mathrm{nl}}\right) \geqslant \wp^*\left(\sigma_{A'B'}; \mathsf{G}_{\mathrm{nl}}\right)$, for all nonlocal games G_{nl}.

The above definition can be equivalently reformulated in terms of Bell inequalities [2] as follows. Since it is known that to any nonlocal game there corresponds a Bell inequality and, conversely, to any Bell inequality there corresponds a nonlocal game [12], we can equivalently say that $\varrho_{AB} \succcurlyeq_{\mathrm{nl}} \sigma_{A'B'}$, if and only if ϱ_{AB} appears to be more nonlocal than $\sigma_{A'B'}$ with respect to all Bell inequalities (or, more precisely speaking, all Bell expressions [13]).

Local operations and shared randomness.—Let us now turn to the LOSR paradigm within quantum theory (again, we begin with the bipartite case): a completely positive trace-preserving (CPTP) map $\mathcal{E} : \mathsf{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathsf{L}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ is said to be an LOSR transformation, if it can be written as $\sum_i \nu(i)\mathcal{E}^i \otimes \mathcal{F}^i$, where $\mathcal{E}^i : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathcal{H}_{A'})$ and $\mathcal{F}^i : \mathsf{L}(\mathcal{H}_B) \to \mathsf{L}(\mathcal{H}_{B'})$ are CPTP maps for all i, and $\nu(i)$ is a probability distribution [14]. We then introduce the following definition:

Definition 3. A bipartite state $\varrho_{AB} \in \mathsf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be *LOSR sufficient* for another bipartite state $\sigma_{A'B'} \in \mathsf{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, written $\varrho_{AB} \dashrightarrow \sigma_{A'B'}$, if and only if there exists an LOSR transformation mapping ϱ_{AB} into $\sigma_{A'B'}$.

It is a rather straightforward exercise to prove that the relation $\dashrightarrow$ implies the relation $\succcurlyeq_{\text{nl}}$. In fact, $\varrho_{AB} \succcurlyeq_{\text{nl}} (\mathcal{E}^i \otimes \mathcal{F}^i)\varrho_{AB}$ trivially holds for all i. On the other hand, the payoff achievable with the convex combination $\sum_i \nu(i)(\mathcal{E}^i \otimes \mathcal{F}^i)\varrho_{AB}$ cannot exceed the best payoff achievable with each of its component, i.e. there exists i such that $(\mathcal{E}^i \otimes \mathcal{F}^i)\varrho_{AB} \succcurlyeq_{\text{nl}} \sum_i \nu(i)(\mathcal{E}^i \otimes \mathcal{F}^i)\varrho_{AB}$. This proves the claim.

It is also straightforward to prove that separable states are the endpoints of the relation $\dashrightarrow$, i.e. for any separable state $\sigma_{A'B'}$, $\varrho_{AB} \dashrightarrow \sigma_{A'B'}$, for all ϱ_{AB}. Suppose, in fact, that $\sigma_{A'B'} \in \mathsf{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ is a separable state, i.e., $\sigma_{A'B'} = \sum_i \nu(i)\gamma^i_{A'} \otimes \chi^i_{B'}$, for some probability distribution $\nu(i)$ and some local states $\gamma^i \in \mathsf{S}(\mathcal{H}_{A'})$ and $\chi^i \in \mathsf{S}(\mathcal{H}_{B'})$. Then, there always exists a "discard-and-prepare" LOSR map $\mathcal{E} : \mathsf{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathsf{L}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ such that $\sigma_{A'B'} = \mathcal{E}(\varrho_{AB})$, for all $\varrho_{AB} \in \mathsf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, proving the claim.

These two facts together make it easy to verify that, in any nonlocal game G_{nl}, all separable states yield exactly the same payoff $\wp_{\text{sep}}(\mathsf{G}_{\text{nl}})$. This remark will be useful in what follows.

Semi-quantum nonlocal games.—At this point, the question of whether the implication can be reversed, i.e. whether the relation $\succcurlyeq_{\text{nl}}$ implies $\dashrightarrow$ or not, naturally arises, and its answer is "no". Let us consider in fact those entangled quantum states (called LHVPOV states [4]) for which a local-hidden-variable model exists, describing the outcome statistics of every local POVM measurement performed on them. This means that, for any nonlocal game G_{nl}, the expected payoff obtainable from such entangled states never exceeds that obtainable from separable states. However, it is impossible to create an entangled state (even if LHVPOV) by acting with LOSR transformations on separable states. This proves the claim that $\succcurlyeq_{\text{nl}}$ does not imply $\dashrightarrow$.

The relation $\succcurlyeq_{\text{nl}}$ is too weak to imply $\dashrightarrow$. We hence introduce a stronger version of $\succcurlyeq_{\text{nl}}$, by suitably enlarging the set of nonlocal games we consider. The extended notion of nonlocal games we need is the following:

Definition 4. The rules of a *semi-quantum nonlocal game* G_{sq} consist of: four index sets $\mathcal{S} = \{s\}$, $\mathcal{T} = \{t\}$, $\mathcal{X} = \{x\}$, and $\mathcal{Y} = \{y\}$; two quantum systems A_0 and B_0; two random sources $\tau = (\{p(s), \tau^s\}; s \in \mathcal{S})$ and $\omega = (\{q(t), \omega^t\}; t \in \mathcal{T})$ on A_0 and B_0, respectively; a payoff function $\wp : \mathcal{S} \times \mathcal{T} \times \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$. A referee picks indices $s \in \mathcal{S}$ and $t \in \mathcal{T}$ at random with probabilities $p(s)$ and $q(t)$, and sends the corresponding states τ^s and ω^t to Alice and Bob, respectively (without revealing the actual indices s and t though). The two players, without communicating with each other, must compute answers $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively, and send them to the referee, who will then pay them both an amount equal to $\wp(s, t, x, y)$.

In other words, while in conventional nonlocal games the referee asks the players "classical" questions, in semi-quantum nonlocal games the referee is allowed to ask them "quantum" questions. Clearly, semi-quantum nonlocal games contain, as special cases, conventional nonlocal games (Def. 1), whenever the states that the referee sends to Alice and Bob are perfectly distinguishable, i.e. "classical". The situation is depicted in Figure 1.

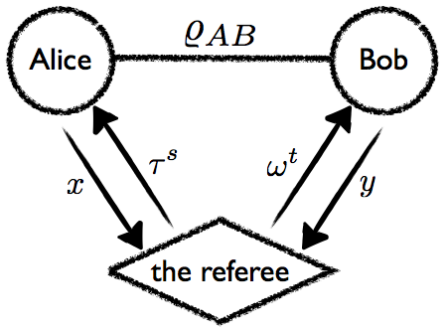

FIG. 1. In a semi-quantum nonlocal game (Def. 4), while players still reply with "classical" answers, the referee is allowed to ask "quantum" questions. Whenever the signals τ^s and ω^t are perfectly distinguishable, i.e. classical, the case of conventional nonlocal games (Def. 1) is recovered. By means of semi-quantum nonlocal games, it is possible to show that all entangled quantum states are nonlocal (Cor. 1).

As in the case of conventional nonlocal games, the two players are allowed to share a bipartite quantum state, say ϱ_{AB}, so that the expected payoff $\wp^*(\varrho_{AB}; \mathsf{G}_{\text{sq}})$ is given by the same formula (1), the only difference being that the joint conditional probability distribution $\mu(x, y|s, t)$ is now computed as

$$\text{Tr}\left[(P^x_{A_0A} \otimes Q^y_{BB_0})(\tau^s_{A_0} \otimes \varrho_{AB} \otimes \omega^t_{B_0})\right].$$

Analogously to what was done before, we can compare the nonlocal utility of two quantum states for *all* semi-quantum nonlocal games and introduce the following relation:

Definition 5. Given two bipartite states $\varrho_{AB} \in \mathsf{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_{A'B'} \in \mathsf{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$, we define the relation $\varrho_{AB} \succcurlyeq_{\text{sq}} \sigma_{A'B'}$, meaning that $\wp^*(\varrho_{AB}; \mathsf{G}_{\text{sq}}) \geqslant \wp^*(\sigma_{A'B'}; \mathsf{G}_{\text{sq}})$, for all semi-quantum nonlocal games G_{sq}.

Since semi-quantum nonlocal games contain conventional nonlocal games as a special case, the relation $\succcurlyeq_{\text{sq}}$ implies the relation $\succcurlyeq_{\text{nl}}$. Moreover, along the same line of thoughts used above to show that $\dashrightarrow$ implies $\succcurlyeq_{\text{nl}}$, it is straightforward to prove that $\dashrightarrow$ also implies $\succcurlyeq_{\text{sq}}$.

A fundamental equivalence.—We are now ready to state the main result of this letter:

Proposition 1. *Given two bipartite states ϱ_{AB} and $\sigma_{A'B'}$, $\varrho_{AB} \succcurlyeq_{\text{sq}} \sigma_{A'B'}$ if and only if $\varrho_{AB} \dashrightarrow \sigma_{A'B'}$.*

The proof of Prop. 1 is based on arguments very similar to those used in Ref. [15], and crucially uses the Separation Theorem between convex sets [16]. Being rather technical in nature, we omit it here, pointing the interested reader to the supplemental material accompanying this letter [17]. Here we only discuss one important consequence of our main result, that is, Prop. 1 implies that *any entangled state is strictly more nonlocal than every separable state*, as stated in the following corollary:

Corollary 1. *In any semi-quantum nonlocal game* G_{sq}*, all separable quantum states yield exactly the same payoff* $\wp_{\mathrm{sep}}(\mathsf{G}_{\mathrm{sq}})$*. Moreover, a quantum state* ϱ_{AB} *is entangled if and only if there exists a semi-quantum nonlocal game* G_{sq}*, for which* $\wp^*(\varrho_{AB};\mathsf{G}_{\mathrm{sq}}) > \wp_{\mathrm{sep}}(\mathsf{G}_{\mathrm{sq}})$.

In other words, any entangled quantum state has a form of nonlocality, which is "hidden" [11] for conventional nonlocal games (and hence Bell inequalities), but becomes apparent when playing semi-quantum nonlocal games. The proof of the above corollary is a direct consequence of the fact that separable states, being the endpoints of the relation $\dashrightarrow$, are also the endpoints of the relation $\succcurlyeq_{\mathrm{sq}}$, due to the equivalence established by Prop. 1.

An example.—In order to illustrate the superiority of semi-quantum nonlocal games, with respect to conventional ones, in witnessing entanglement, we describe now the example of a semi-quantum nonlocal game, in which every entangled state gives rise to joint question-answer probability distributions that cannot be explained as coming from *any* separable state, even if supplemented with an unlimited amount of shared randomness. This is true also for entangled LHVPOV states, which are instead completely indistinguishable from separable states, if only conventional nonlocal games (Def. 1) are considered. The example, directly stemming from the proof of Proposition 1 (see [17]), is described here only in the case of two-qubit states; we remark, however, that the same construction can be easily carried over to any finite dimensional case.

In our example, $\mathcal{S} = \mathcal{T} = \mathcal{X} = \mathcal{Y} = \{1,2,3,4\}$, the auxiliary quantum systems used by the referee to encode her questions are represented by two qubits, i.e. $\mathcal{H}_{A_0} \cong \mathcal{H}_{B_0} \cong \mathbb{C}^2$, and the "question states" are the four tetrahedral states $|\psi^1\rangle$, $|\psi^2\rangle$, $|\psi^3\rangle$, and $|\psi^4\rangle$ defined by Davies [18]. Notice that the choice of the question states is somewhat arbitrary: the important point is that their density matrices constitute a basis for the linear space $\mathsf{L}(\mathbb{C}^2)$. (The definition of the probability distributions on $\mathcal{S}$ and $\mathcal{T}$, as well as that of the payoff function, are not necessary for our argument and can be omitted.)

Given a two-qubit state ϱ_{AB}, let us consider the joint conditional question-answer probability distribution $\bar{\mu}(x,y|s,t\|\varrho)$ computed as

$$\mathrm{Tr}\left[(B^x_{A_0A} \otimes B^y_{BB_0})(\psi^s_{A_0} \otimes \varrho_{AB} \otimes \psi^t_{B_0})\right], \qquad (2)$$

where B^1, B^2, B^3, B^4 are, respectively, the four orthogonal Bell measurements on $\Phi^+, \Phi^-, \Psi^+, \Psi^-$. In the process of proving Prop. 1 (see [17]), it is also shown that, in particular, the two-qubit state ϱ_{AB} is entangled if and only if, for any (possibly higher-dimensional) separable state $\sigma_{A'B'}$ and for any possible POVMs $P \in \mathscr{M}(A_0A';\mathcal{X})$ and $Q \in \mathscr{M}(B'B_0;\mathcal{Y})$,

$$\bar{\mu}(x,y|s,t\|\varrho) \neq \mathrm{Tr}\left[(P^x_{A_0A'} \otimes Q^y_{B'B_0})(\psi^s_{A_0} \otimes \sigma_{A'B'} \otimes \psi^t_{B_0})\right].$$

In fact, one can easily check, following the proof of Prop. 1, that an equality in the above equation, for some separable state $\sigma_{A'B'}$ and some POVMs P and Q, would imply the existence of an LOSR transformation mapping $\sigma_{A'B'}$ into ϱ_{AB}, hence leading to a contradiction, due to the fact that LOSR transformations cannot create entangled states from separable ones. In other words, the state ϱ_{AB} is entangled if and only if the joint conditional probability distribution $\bar{\mu}(x,y|s,t\|\varrho)$, computed in Eq. (2), is out of reach for any possible separable state, even with the help of unlimited shared randomness (represented here by the possibility of $\sigma_{A'B'}$ being on a higher-dimensional Hilbert space).

Multipartite states.—Before concluding, we remark here that our approach can be straightforwardly extended to consider multipartite LOSR transformations $\mathcal{E} : \mathsf{L}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \cdots) \to \mathsf{L}(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_{C'} \otimes \cdots)$ of the form $\mathcal{E} = \sum_i \nu(i)\mathcal{E}^i \otimes \mathcal{F}^i \otimes \mathcal{G}^i \otimes \cdots$, where $\mathcal{E}^i : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathcal{H}_{A'})$, $\mathcal{F}^i : \mathsf{L}(\mathcal{H}_B) \to \mathsf{L}(\mathcal{H}_{B'})$, $\mathcal{G}^i : \mathsf{L}(\mathcal{H}_C) \to \mathsf{L}(\mathcal{H}_{C'})$, and so on, are all CPTP maps, for all i. This can be done by considering multipartite semi-quantum nonlocal games, in which all the players independently receive their "quantum questions" from the referee, and by following the same arguments used to prove the bipartite case.

Conclusions.—We showed that one quantum state can be transformed into another by means of an LOSR protocol, if and only if the former is "more nonlocal" than the latter, where nonlocality is quantified by means of semi-quantum nonlocal games (Def. 5). As a by-product, we obtained a clear-cut proof that *any entangled quantum state is always nonlocal*, a fact that should be considered in light of previous works reaching the same conclusion, although from very different routes [11]. In order to support our analysis and show the superiority of semi-quantum nonlocal games, with respect to conventional ones, in witnessing entanglement, we also provided an explicit example of a semi-quantum nonlocal game, in which any entangled state gives rise to joint question-answer probability distributions that cannot be explained classically, even if an unlimited amount of shared randomness is granted.

Acknowledgments.—The author is grateful to Denis Rosset and Mark M. Wilde for pointing out mistakes in

a previous version. An exchange with Antonio Acín and Miguel Navascués is also gratefully acknowledged. This research was supported by the Program for Improvement of Research Environment for Young Researchers from Special Coordination Funds for Promoting Science and Technology (SCF) commissioned by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan.

* buscemi@iar.nagoya-u.ac.jp

[1] A. Einstein, B. Podolsky, and N. Rosen,Phys. Rev. **47**, 777 (1935).
[2] J. S. Bell, Physics **1**, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[3] R. F. Werner, Phys. Rev. A **40**, 4277 (1989); N. Gisin, Phys. Lett. A **154**, 201 (1991); R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).
[4] J. Barrett, Phys. Rev. A **65**, 042302 (2002).
[5] A. A. Méthot and V. Scarani, Quant. Inf. Comp. **7**, 157 (2007).
[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K Wootters, Phys. Rev. A **54**, 3824 (1996).
[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[8] D. D. Dukaric and S. Wolf, arXiv:0808.3317v2; M. Forster, S. Winkler, and S. Wolf, Phys. Rev. Lett. **102**, 120401 (2009); M. Forster and S. Wolf, Phys. Rev. A **84**, 042112 (2011).
[9] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, arXiv:1112.2647v1.
[10] A. J. Short, S. Popescu, and N. Gisin, Phys. Rev. A **73**, 012101 (2006).
[11] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995); N. Gisin, Phys. Lett. A **210**, 151 (1996); A. Peres, Phys. Rev. A **54**, 2685 (1996); L. Masanes, Y.-C. Liang, and A. C. Doherty, Phys. Rev. Lett. **100**, 090403 (2008).
[12] J. Silman, S. Machnes, and N. Aharon, Phys. Lett. A **372**, 3796 (2008).
[13] T. Vértesi and E. Bene, Phys. Rev. A **82**, 062115 (2010).
[14] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, Phys. Rev. A **64**, 052309 (2001).
[15] F. Buscemi, Commun. Math. Phys. **310**, 625 (2012).
[16] R. T. Rockafellar, *Convex Analysis* (Princeton University Press, Princeton, 1970), Corollary 11.4.2 therein.
[17] See the Supplemental Material at [...] for the proof of Proposition 1.
[18] E. B. Davies, IEEE Trans. Inf. Th. **24**, 596 (1978). Proof of Proposition 8 therein.

Supplemental Material

Remark. The numbering of equations and references follows that given in the main text.

Remark. In what follows, for notational convenience, the density matrices τ^s and ω^t are taken sub-normalized, so that $\mathrm{Tr}[\tau^s] = p(s)$ and $\mathrm{Tr}[\omega^t] = q(t)$.

Proof of Proposition 1. We explicitly prove only the non-trivial direction, i.e. the "only if" part of the statement.

We start by making the following observation: the payoff function $\wp^*(\varrho_{AB}; \mathsf{G}_{\mathrm{sq}})$ contains a maximization over local measurements $P \in \mathscr{M}(A_0 A; \mathcal{X})$ and $Q \in \mathscr{M}(BB_0; \mathcal{Y})$ on Alice's and Bob's systems, respectively. The set of local measurements does not constitute a convex set, in the sense that a convex combination $p(P' \otimes Q') + (1-p)(P'' \otimes Q'')$, for $P', P'' \in \mathscr{M}(A_0 A; \mathcal{X})$ and $Q', Q'' \in \mathscr{M}(BB_0; \mathcal{Y})$, in general cannot be written as $P \otimes Q$, for any $P \in \mathscr{M}(A_0 A; \mathcal{X})$ and $Q \in \mathscr{M}(BB_0; \mathcal{Y})$. However, since the function

$$g(\varrho_{AB}; \mathsf{G}_{\mathrm{sq}}; P, Q) := \sum_{s,t,x,y} \wp(s,t,x,y)\ \mathrm{Tr}\left[\left(P^x_{A_0 A} \otimes Q^y_{BB_0}\right)\ \left(\tau^s_{A_0} \otimes \varrho_{AB} \otimes \omega^t_{B_0}\right)\right]$$

is linear in the POVMs P and Q, we can extend it by linearity to any convex combination $\sum_i \nu(i) P^x_{A_0 A}(i) \otimes Q^y_{BB_0}(i)$, where $\nu(i)$ are probabilities and $P(i) \in \mathscr{M}(A_0 A; \mathcal{X})$ and $Q(i) \in \mathscr{M}(BB_0; \mathcal{Y})$, for all i. Let us denote by $\mathsf{Co}\{\mathscr{M}(A_0 A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}$ the set of such convex combinations of local POVMs.

Since a linear function is, in particular, convex; since a convex function on a convex set achieves its maximum on the extremal points of such set; and since the extremal points of $\mathsf{Co}\{\mathscr{M}(A_0 A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}$ are, by construction, local POVMs, we have that

$$\max_{Z \in \mathsf{Co}\{\mathscr{M}(A_0 A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}} g(\varrho_{AB}; \mathsf{G}_{\mathrm{sq}}; Z) = \wp^*(\varrho_{AB}; \mathsf{G}_{\mathrm{sq}}). \tag{3}$$

For any choice of $\mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega$ (the meaning of the notation is the same as in Def. 4), let us now consider the set of probability distributions defined as follows :

$$\mathscr{P}(\varrho_{AB}; \mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega) := \left\{ \mu \in \mathscr{P}(\mathcal{S} \times \mathcal{T} \times \mathcal{X} \times \mathcal{Y}) \,\middle|\, \begin{array}{l} \mu(s,t,x,y) = \mathrm{Tr}\left[Z^{x,y}_{A_0 A B B_0}\ \left(\tau^s_{A_0} \otimes \varrho_{AB} \otimes \omega^t_{B_0}\right)\right], \\ Z \in \mathsf{Co}\{\mathscr{M}(A_0 A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\} \end{array} \right\}.$$

Due to the identity (3), we have that

$$\wp^*(\varrho_{AB}; \mathsf{G}_{\mathrm{sq}}) = \max_{\mu \in \mathscr{P}(\varrho_{AB}; \mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega)} \sum_{s,t,x,y} \mu(s,t,x,y) \wp(s,t,x,y).$$

The crucial point, now, is that, by construction, the set $\mathscr{P}(\varrho_{AB}; \mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega)$ is convex, as it inherits the convex structure from $\mathsf{Co}\{\mathscr{M}(A_0 A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}$. Therefore, following the same arguments presented in more detail in [15], as a consequence of the so-called "separation theorem" for convex sets [16], Def. 5 can be reformulated in the following way:

$$\varrho_{AB} \succcurlyeq_{\mathrm{sq}} \sigma_{A'B'} \quad \Leftrightarrow \quad \mathscr{P}(\varrho_{AB}; \mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega) \supseteq \mathscr{P}(\sigma_{A'B'}; \mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega),$$

for any choice of $\mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega$.

More explicitly stated, $\varrho_{AB} \succcurlyeq_{\mathrm{sq}} \sigma_{A'B'}$ if and only if, for any choice of $\mathcal{S}, \mathcal{T}, \mathcal{X}, \mathcal{Y}, A_0, B_0, \tau, \omega$, and for any POVM $Z \in \mathsf{Co}\{\mathscr{M}(A_0 A'; \mathcal{X}) \otimes \mathscr{M}(B' B_0; \mathcal{Y})\}$, there exists a POVM $\bar{Z} \in \mathsf{Co}\{\mathscr{M}(A_0 A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}$, such that

$$\mathrm{Tr}\left[\bar{Z}^{x,y}_{A_0 A B B_0}\ \left(\tau^s_{A_0} \otimes \varrho_{AB} \otimes \omega^t_{B_0}\right)\right] = \mathrm{Tr}\left[Z^{x,y}_{A_0 A' B' B_0}\ \left(\tau^s_{A_0} \otimes \sigma_{A'B'} \otimes \omega^t_{B_0}\right)\right], \tag{4}$$

for all $s \in \mathcal{S}$, $t \in \mathcal{T}$, $x \in \mathcal{X}$, and $y \in \mathcal{Y}$.

Let us now choose A_0 and B_0 to be such that $\mathcal{H}_{A_0} \cong \mathcal{H}_{A'}$ and $\mathcal{H}_{B_0} \cong \mathcal{H}_{B'}$. Moreover, let us introduce two further auxiliary quantum systems A_1 and B_1, with $\mathcal{H}_{A_1} \cong \mathcal{H}_{A_0}$ ($\cong \mathcal{H}_{A'}$) and $\mathcal{H}_{B_1} \cong \mathcal{H}_{B_0}$ ($\cong \mathcal{H}_{B'}$). Next, let us choose $(\tau^s; s \in \mathcal{S})$ on A_0 to be given by

$$\tau^s_{A_0} = \mathrm{Tr}_{A_1}\left[\left(\Theta^s_{A_1} \otimes \mathbb{1}_{A_0}\right)\ \Psi^+_{A_1 A_0}\right],$$

and $(\omega^t; t \in \mathcal{T})$ on B_0 by

$$\omega^t_{B_0} = \mathrm{Tr}_{B_1}\left[\left(\mathbb{1}_{B_0} \otimes \Upsilon^t_{B_1}\right)\ \Psi^+_{B_0B_1}\right],$$

where Ψ^+ denotes a maximally entangled state and the two POVMs $\Theta \in \mathscr{M}(A_1; \mathcal{S})$ and $\Upsilon \in \mathscr{M}(B_1; \mathcal{T})$ are both informationally complete (i.e. their linear span coincide with $\mathsf{L}(\mathcal{H}_{A_1})$ and $\mathsf{L}(\mathcal{H}_{B_1})$, respectively). Then, Eq. (4) can be written as

$$\begin{aligned}&\mathrm{Tr}\left[\left(\Theta^s_{A_1} \otimes \bar{Z}^{x,y}_{A_0ABB_0} \otimes \Upsilon^t_{B_1}\right)\ \left(\Psi^+_{A_1A_0} \otimes \varrho_{AB} \otimes \Psi^+_{B_0B_1}\right)\right]\\ =&\mathrm{Tr}\left[\left(\Theta^s_{A_1} \otimes Z^{x,y}_{A_0A'B'B_0} \otimes \Upsilon^t_{B_1}\right)\ \left(\Psi^+_{A_1A_0} \otimes \sigma_{A'B'} \otimes \Psi^+_{B_0B_1}\right)\right],\end{aligned}$$

for all s, t, x, y.

Due to the fact that the POVMs Θ and Υ have been chosen to be informationally complete, we arrive at the following conclusion: if $\varrho_{AB} \succcurlyeq_{\mathrm{sq}} \sigma_{A'B'}$, then, for any choice of outcome sets $\mathcal{X}, \mathcal{Y}$ and POVMs $P \in \mathscr{M}(A_0A'; \mathcal{X})$ and $Q \in \mathscr{M}(B'B_0; \mathcal{Y})$, there exists a POVM $\bar{Z} \in \mathsf{Co}\{\mathscr{M}(A_0A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}$, such that

$$\begin{aligned}&\mathrm{Tr}_{A_0ABB_0}\left[\left(\mathbb{1}_{A_1} \otimes \bar{Z}^{x,y}_{A_0ABB_0} \otimes \mathbb{1}_{B_1}\right)\ \left(\Psi^+_{A_1A_0} \otimes \varrho_{AB} \otimes \Psi^+_{B_0B_1}\right)\right]\\ =&\mathrm{Tr}_{A_0A'B'B_0}\left[\left(\mathbb{1}_{A_1} \otimes P^x_{A_0A'} \otimes Q^y_{B'B_0} \otimes \mathbb{1}_{B_1}\right)\ \left(\Psi^+_{A_1A_0} \otimes \sigma_{A'B'} \otimes \Psi^+_{B_0B_1}\right)\right],\end{aligned} \tag{5}$$

for all $x \in \mathcal{X}$ and all $y \in \mathcal{Y}$.

Let us now choose $\mathcal{X}$ and $\mathcal{Y}$ such that $|\mathcal{X}| = (\dim \mathcal{H}_{A'})^2$ and $|\mathcal{Y}| = (\dim \mathcal{H}_{B'})^2$, and the POVMs P and Q to be the generalized Bell measurements on A_0A' and $B'B_0$, respectively. With this choice in mind, let us denote the right-hand side of (5) by $\sigma^{x,y}_{A_1B_1}$. The protocol of quantum teleportation provides unitary operators $U^x : \mathcal{H}_{A_1} \to \mathcal{H}_{A'}$ and $V^y : \mathcal{H}_{B_1} \to \mathcal{H}_{B'}$ such that

$$\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} \left(U^x_{A_1} \otimes V^y_{B_1}\right) \sigma^{x,y}_{A_1B_1} \left(U^x_{A_1} \otimes V^y_{B_1}\right)^\dagger = \sigma_{A'B'}.$$

On the other hand, since $\varrho_{AB} \succcurlyeq_{\mathrm{sq}} \sigma_{A'B'}$, via equation (5), we know that there exists a POVM $\bar{Z} \in \mathsf{Co}\{\mathscr{M}(A_0A; \mathcal{X}) \otimes \mathscr{M}(BB_0; \mathcal{Y})\}$, such that

$$\begin{aligned}&\sigma_{A'B'}\\ =&\sum_{x,y} \left(U^x_{A_1} \otimes V^y_{B_1}\right) \mathrm{Tr}_{A_0ABB_0}\left[\left(\mathbb{1}_{A_1} \otimes \bar{Z}^{x,y}_{A_0ABB_0} \otimes \mathbb{1}_{B_1}\right)\ \left(\Psi^+_{A_1A_0} \otimes \varrho_{AB} \otimes \Psi^+_{B_0B_1}\right)\right] \left(U^x_{A_1} \otimes V^y_{B_1}\right)^\dagger.\end{aligned} \tag{6}$$

Finally, by expanding the POVM elements $\bar{Z}^{x,y}_{A_0ABB_0}$ into a convex combination $\bar{Z}^{x,y}_{A_0ABB_0} = \sum_i \nu(i) \bar{P}^x_{A_0A}(i) \otimes \bar{Q}^y_{BB_0}(i)$, where $\bar{P}(i) \in \mathscr{M}(A_0A; \mathcal{X})$ and $\bar{Q}(i) \in \mathscr{M}(BB_0; \mathcal{Y})$ for all i, and by defining CPTP maps $\mathcal{E}^i(z) : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathcal{H}_{A'})$ and $\mathcal{F}^i(w) : \mathsf{L}(\mathcal{H}_B) \to \mathsf{L}(\mathcal{H}_{B'})$ as

$$\mathcal{E}^i(z_A) := \sum_{x\in\mathcal{X}} U^x_{A_1}\ \mathrm{Tr}_{A_0A}\left[\left(\mathbb{1}_{A_1} \otimes \bar{P}^x_{A_0A}(i)\right)\ \left(\Psi^+_{A_1A_0} \otimes z_A\right)\right] \left(U^x_{A_1}\right)^\dagger$$

and

$$\mathcal{F}^i(w_B) := \sum_{y\in\mathcal{Y}} V^y_{B_1}\ \mathrm{Tr}_{B_0B}\left[\left(\bar{Q}^y_{BB_0}(i) \otimes \mathbb{1}_{B_1}\right)\ \left(w_B \otimes \Psi^+_{B_0B_1}\right)\right] \left(V^y_{B_1}\right)^\dagger,$$

Eq. (6) can be rewritten as $\sigma_{A'B'} = \sum_i \nu(i)(\mathcal{E}^i_A \otimes \mathcal{F}^i_B)(\varrho_{AB})$. This concludes the proof. ∎